

Contents

Preface to the Second Edition	xiii
Preface to the First Edition	xvii
I Getting Started	1
1 Introduction	3
1.1 Security Truisms	3
1.2 Picking a Security Policy	7
1.2.1 Policy Questions	7
1.2.2 Stance	9
1.3 Host-Based Security	10
1.4 Perimeter Security	10
1.5 Strategies for a Secure Network	11
1.5.1 Host Security	11
1.5.2 Gateways and Firewalls	13
1.5.3 DMZs	14
1.5.4 Encryption—Communications Security	15
1.6 The Ethics of Computer Security	16
1.7 WARNING	18
2 A Security Review of Protocols: Lower Layers	19
2.1 Basic Protocols	19
2.1.1 IP	20
IP Addresses	21
2.1.2 ARP	22
2.1.3 TCP	22
TCP Open	23
TCP Sessions	24
2.1.4 SCTP	25
2.1.5 UDP	27

2.1.6	ICMP	27
2.2	Managing Addresses and Names	28
2.2.1	Routers and Routing Protocols	28
BGP	30	
2.2.2	The Domain Name System	31
DNSsec	33	
2.2.3	BOOTP and DHCP	33
2.3	IP version 6	34
2.3.1	IPv6 Address Formats	35
2.3.2	Neighbor Discovery	36
2.3.3	DHCPv6	36
2.3.4	Filtering IPv6	36
2.4	Network Address Translators	37
2.5	Wireless Security	38
2.5.1	Fixing WEP	39
3	Security Review: The Upper Layers	41
3.1	Messaging	41
3.1.1	SMTP	41
3.1.2	MIME	43
3.1.3	POP version 3	44
3.1.4	IMAP Version 4	45
3.1.5	Instant Messaging	45
3.2	Internet Telephony	46
3.2.1	H.323	46
3.2.2	SIP	47
3.3	RPC-Based Protocols	47
3.3.1	RPC and Rpcbind	47
3.3.2	NIS	50
3.3.3	NFS	51
3.3.4	Andrew	52
3.4	File Transfer Protocols	52
3.4.1	TFTP	52
3.4.2	FTP	53
3.4.3	SMB Protocol	57
3.5	Remote Login	58
3.5.1	Telnet	58
3.5.2	The “r” Commands	59
3.5.3	Ssh	61
3.6	Simple Network Management Protocol—SNMP	62
3.7	The Network Time Protocol	63
3.8	Information Services	64
3.8.1	Finger: Looking Up People	64

3.8.2	Whois—Database Lookup Service	64
3.8.3	LDAP	65
3.8.4	World Wide Web	65
3.8.5	NNTP—Network News Transfer Protocol	66
3.8.6	Multicasting and the MBone	67
3.9	Proprietary Protocols	68
3.9.1	RealAudio	68
3.9.2	Oracle's SQL*Net	68
3.9.3	Other Proprietary Services	69
3.10	Peer-to-Peer Networking	69
3.11	The X11 Window System	70
3.11.1	xdm	71
3.12	The Small Services	71
4	The Web: Threat or Menace?	73
4.1	The Web Protocols	74
4.1.1	HTTP	74
	Maintaining Connection State	76
4.1.2	SSL	77
4.1.3	FTP	77
4.1.4	URLs	78
4.2	Risks to the Clients	79
4.2.1	ActiveX	80
4.2.2	Java and Applets	80
4.2.3	JavaScript	82
4.2.4	Browsers	83
4.3	Risks to the Server	85
4.3.1	Access Controls	85
4.3.2	Server-Side Scripts	86
4.3.3	Securing the Server Host	86
4.3.4	Choice of Server	87
4.4	Web Servers vs. Firewalls	89
4.5	The Web and Databases	91
4.6	Parting Thoughts	91

II The Threats 93

5	Classes of Attacks	95
5.1	Stealing Passwords	95
5.2	Social Engineering	98
5.3	Bugs and Back Doors	100
5.4	Authentication Failures	103

5.4.1	Authentication Races	104
5.5	Protocol Failures	104
5.6	Information Leakage	105
5.7	Exponential Attacks—Viruses and Worms	106
5.8	Denial-of-Service Attacks	107
5.8.1	Attacks on a Network Link	108
5.8.2	Attacking the Network Layer	108
Killer and ICMP Packets	108	
SYN Packet Attacks	109	
Application-Level Attacks—Spam	109	
5.8.3	DDoS	110
5.8.4	What to Do About a Denial-of-Service Attack	111
Filter Out the Bad Packets	111	
Improve the Processing Software	114	
Hunt Them Down Like Dogs	114	
Increase the Capacity of the Target	116	
5.8.5	Backscatter	116
5.9	Botnets	117
5.10	Active Attacks	117
6	The Hacker's Workbench, and Other Munitions	119
6.1	Introduction	119
6.2	Hacking Goals	121
6.3	Scanning a Network	121
6.4	Breaking into the Host	122
6.5	The Battle for the Host	123
6.5.1	Setuid <i>root</i> Programs	124
6.5.2	Rootkit	125
6.6	Covering Tracks	126
6.6.1	Back Doors	127
6.7	Metastasis	127
6.8	Hacking Tools	128
6.8.1	Crack—Dictionary Attacks on UNIX Passwords	129
6.8.2	<i>Dsniff</i> —Password Sniffing Tool	129
6.8.3	<i>Nmap</i> —Find and Identify Hosts	130
6.8.4	<i>Nbaudit</i> —Check NetBIOS Share Information	130
6.8.5	<i>Juggernaut</i> —TCP Hijack Tool	130
6.8.6	<i>Nessus</i> —Port Scanning	131
6.8.7	DDoS Attack Tools	131
6.8.8	Ping of Death—Issuing Pathological Packets	131
6.8.9	Virus Construction Kits	131
6.8.10	Other Tools	132
6.9	Tiger Teams	132


III	Safer Tools and Services	135
7	Authentication	137
7.1	Remembering Passwords	138
7.1.1	Rolling the Dice	142
7.1.2	The Real Cost of Passwords	143
7.2	Time-Based One-Time Passwords	144
7.3	Challenge/Response One-Time Passwords	145
7.4	Lamport's One-Time Password Algorithm	146
7.5	Smart Cards	147
7.6	Biometrics	147
7.7	RADIUS	148
7.8	SASL: An Authentication Framework	149
7.9	Host-to-Host Authentication	149
7.9.1	Network-Based Authentication	149
7.9.2	Cryptographic Techniques	149
7.10	PKI	150
8	Using Some Tools and Services	153
8.1	<i>Inetd</i> —Network Services	153
8.2	<i>Ssh</i> —Terminal and File Access	154
8.2.1	Single-Factor Authentication for <i>ssh</i>	154
8.2.2	Two-Factor Authentication	157
8.2.3	Authentication Shortcomings	157
8.2.4	Server Authentication	158
8.3	<i>Syslog</i>	158
8.4	Network Administration Tools	159
8.4.1	Network Monitoring	159
8.4.2	Using <i>Tcpdump</i>	159
8.4.3	Ping, <i>Traceroute</i> , and <i>Dig</i>	160
8.5	<i>Chroot</i> —Caging Suspect Software	162
8.6	Jailing the Apache Web Server	165
8.6.1	CGI Wrappers	166
8.6.2	Security of This Web Server	167
8.7	<i>Aftpd</i> —A Simple Anonymous FTP Daemon	167
8.8	Mail Transfer Agents	168
8.8.1	Postfix	168
8.9	POP3 and IMAP	168
8.10	Samba: An SMB Implementation	169
8.11	Taming <i>Named</i>	170
8.12	Adding SSL Support with <i>Sslwrap</i>	170

IV	Firewalls and VPNs	173
9	Kinds of Firewalls	175
9.1	Packet Filters	176
9.1.1	Network Topology and Address-Spoofing	179
9.1.2	Routing Filters	182
9.1.3	Sample Configurations	184
9.1.4	Packet-Filtering Performance	185
9.2	Application-Level Filtering	185
9.3	Circuit-Level Gateways	186
9.4	Dynamic Packet Filters	188
9.4.1	Implementation Options	188
9.4.2	Replication and Topology	191
9.4.3	The Safety of Dynamic Packet Filters	193
9.5	Distributed Firewalls	193
9.6	What Firewalls Cannot Do	194
10	Filtering Services	197
10.1	Reasonable Services to Filter	198
10.1.1	DNS	198
10.1.2	Web	202
10.1.3	FTP	202
10.1.4	TCP	202
10.1.5	NTP	203
10.1.6	SMTP/Mail	203
10.1.7	POP3/IMAP	204
10.1.8	<i>ssh</i>	206
10.2	Digging for Worms	206
10.3	Services We Don't Like	207
10.3.1	UDP	207
10.3.2	H.323 and SIP	208
10.3.3	RealAudio	208
10.3.4	SMB	209
10.3.5	X Windows	209
10.4	Other Services	209
10.4.1	IPsec, GRE, and IP over IP	209
10.4.2	ICMP	209
10.5	Something New	210
11	Firewall Engineering	211
11.1	Rulesets	212
11.2	Proxies	214
11.3	Building a Firewall from Scratch	215

11.3.1	Building a Simple, Personal Firewall	216
11.3.2	Building a Firewall for an Organization	220
	<i>Ipfest</i>	226
11.3.3	Application-Based Filtering	226
11.4	Firewall Problems	227
	11.4.1 Inadvertent Problems	227
	11.4.2 Intentional Subversions	228
	11.4.3 Handling IP Fragments	228
	11.4.4 The FTP Problem	229
	11.4.5 Firewalking	229
	11.4.6 Administration	230
11.5	Testing Firewalls	230
	11.5.1 Tiger Teams	231
	11.5.2 Rule Inspection	232
	The Rules	232
	Manual Inspection	232
	Computer-Assisted Inspection	232
12	Tunneling and VPNs	233
12.1	Tunnels	234
	12.1.1 Tunnels Good and Bad	234
12.2	Virtual Private Networks (VPNs)	236
	12.2.1 Remote Branch Offices	237
	12.2.2 Joint Ventures	238
	12.2.3 Telecommuting	239
	Direct Connection to a Company	241
	Connecting Through an ISP	242
	Networking on the Road	242
12.3	Software vs. Hardware	242
	12.3.1 VPN in Software	243
	12.3.2 VPN in Hardware	244
V	Protecting an Organization	245
13	Network Layout	247
	13.1 Intranet Explorations	248
	13.2 Intranet Routing Tricks	249
	13.3 In Host We Trust	253
	13.4 Belt and Suspenders	255
	13.5 Placement Classes	257

14	Safe Hosts in a Hostile Environment	259
14.1	What Do We Mean by “Secure”?	259
14.2	Properties of Secure Hosts	260
14.2.1	Secure Clients	263
	Windows and Macintoshes	263
	Single-User, UNIX-Like Systems	264
	Multi-User Hosts	264
14.2.2	Secure Servers	265
14.2.3	Secure Routers and Other Network Elements	265
14.3	Hardware Configuration	265
14.4	Field-Stripping a Host	266
14.5	Loading New Software	270
14.6	Administering a Secure Host	271
14.6.1	Access	271
14.6.2	Console Access	271
14.6.3	Logging	272
14.6.4	Backup	273
14.6.5	Software Updates	274
14.6.6	Watching the Roost	275
14.7	Skinny-Dipping: Life Without a Firewall	277
15	Intrusion Detection	279
15.1	Where to Monitor	280
15.2	Types of IDSs	281
15.3	Administering an IDS	282
15.4	IDS Tools	282
15.4.1	Snort	282
VI	Lessons Learned	285
16	An Evening with Berferd	287
16.1	Unfriendly Acts	287
16.2	An Evening with Berferd	290
16.3	The Day After	294
16.4	The Jail	295
16.5	Tracing Berferd	296
16.6	Berferd Comes Home	298
17	The Taking of Clark	301
17.1	Prelude	302
17.2	CLARK	302
17.3	Crude Forensics	303

17.4	Examining CLARK	304
17.4.1	/usr/lib	305
17.4.2	/usr/var/tmp	306
17.5	The Password File	310
17.6	How Did They Get In?	310
17.6.1	How Did They Become Root?	311
17.6.2	What Did They Get of Value?	311
17.7	Better Forensics	311
17.8	Lessons Learned	312
18	Secure Communications over Insecure Networks	313
18.1	The Kerberos Authentication System	314
18.1.1	Limitations	316
18.2	Link-Level Encryption	318
18.3	Network-Level Encryption	318
18.3.1	ESP and AH	318
18.3.2	Key Management for IPsec	320
18.4	Application-Level Encryption	322
18.4.1	Remote Login: <i>Ssh</i>	322
18.4.2	SSL—The Secure Socket Layer	323
	Protocol Overview	324
	Security	325
18.4.3	Authenticating SNMP	326
18.4.4	Secure Electronic Mail	326
	S/MIME	326
	PGP	327
18.4.5	Transmission Security vs. Object Security	327
18.4.6	Generic Security Service Application Program Interface	327
19	Where Do We Go from Here?	329
19.1	IPv6	329
19.2	DNSsec	330
19.3	Microsoft and Security	330
19.4	Internet Ubiquity	331
19.5	Internet Security	331
19.6	Conclusion	332
VII	Appendixes	333
A	An Introduction to Cryptography	335
A.1	Notation	335
A.2	Secret-Key Cryptography	337

A.3	Modes of Operation	339
A.3.1	Electronic Code Book Mode	339
A.3.2	Cipher Block Chaining Mode	339
A.3.3	Output Feedback Mode	340
A.3.4	Cipher Feedback Mode	341
A.3.5	Counter Mode	341
A.3.6	One-Time Passwords	342
A.3.7	Master Keys	342
A.4	Public Key Cryptography	342
A.5	Exponential Key Exchange	343
A.6	Digital Signatures	344
A.7	Secure Hash Functions	346
A.8	Timestamps	347
B	Keeping Up	349
B.1	Mailing Lists	350
B.2	Web Resources	351
B.3	Peoples' Pages	352
B.4	Vendor Security Sites	352
B.5	Conferences	353
	Bibliography	355
	List of  s	389
	List of Acronyms	391
	Index	397